International Journal of Science, Technology and Society
2024, Vol. 12, No. 2, pp. 81-87
https://doi.org/10.11648/j.ijsts.20241202.11

Research Article

A Review on Searchable Encryption Functionality and the Evaluation of Homomorphic Encryption

Brian Kishiyama*, Izzat Alsmadi

Department of Computing, Engineering, and Mathematical Sciences, Texas A&M University, San Antonio, The United States

Abstract

Cloud Service Providers, exemplified by industry leaders like Google Cloud Platform, Microsoft Azure, and Amazon Web Services, deliver a dynamic array of cloud services in an ever-evolving landscape. This sector is witnessing substantial growth, with enterprises such as Netflix and PayPal heavily relying on cloud infrastructure for various needs such as data storage, computational resources, and various other services. The adoption of cloud solutions by businesses not only facilitates cost reduction but also fosters flexibility and supports scalability. Despite the undeniable advantages, concerns surrounding security and privacy persist in the realm of Cloud Computing. Given that Cloud services are accessible via the internet, there is a potential vulnerability to unauthorized access by hackers or malicious entities from anywhere in the world. A crucial aspect of addressing this challenge is the implementation of robust security measures, particularly focusing on data protection. To safeguard data in the Cloud, a fundamental recommendation is the encryption of data prior to uploading. Encryption should be maintained consistently, both during storage and in transit. While encryption enhances security, it introduces a potential challenge for data owners who may need to perform various operations on their encrypted data, such as accessing, modifying, updating, deleting, reading, searching, or sharing them with others. One viable solution to balance the need for data security and operational functionality is the adoption of Searchable Encryption (SE). SE operates on encrypted data, allowing authorized users to perform certain operations without compromising the security of sensitive information. The effectiveness of SE has notably advanced since its inception, and ongoing research endeavors aim to further enhance its capabilities. This paper provides a comprehensive review of the functionality of Searchable Encryption, with a primary focus on its applications in Cloud services during the period spanning 2019 to 2023. Additionally, the study evaluates one of its prominent schemes, namely Fully Homomorphic Encryption (FHE). The analysis indicates an overall positive trajectory in SE research, showcasing increased efficiency as multiple functionalities are aggregated and rigorously tested.

Keywords

Security Information, Privacy, Searchable Encryption, Homomorphic Encryption, Cloud Computing

1. Introduction

Cloud computing encompasses a diverse range of re-sources and services, including dedicated virtual machines, core computing, security and identity features, virtual networks, machine learning platforms, cloud storage, and streaming analytics [1].

*Corresponding author: bkishiyama@tamusa.edu (Brian Kishiyama)

Received: 25 February 2024; **Accepted:** 7 March 2024; **Published:** 20 March 2024

Its reach extends to various sectors such as Location Based Services (LBS), Internet of Things (IoTs), Electronic Health (eHealth) research and organizations, blockchains, smart devices, and beyond. Despite the multitude of benefits, the Cloud is not without its challenges, particularly concerning the security and privacy of the data it hosts.

Sensitive information, ranging from personal or customer details to user locations, medical records, and trade secrets, is transmitted to the Cloud by businesses like Netflix, Zoom, and PayPal. The Cloud's accessibility through the Internet makes it susceptible to external threats, including hacking attempts and potential insider threats seeking to exploit valuable trade secrets. Recognizing data as a precious resource necessitates protective measures, and one such measure is data encryption during storage and transit.

While encryption ensures data security, operations on encrypted data, such as searching for files or modifying records, pose a challenge. Traditional solutions involve downloading the entire encrypted database, decryption for operations, re-encryption, and uploading back to the Cloud. However, this approach is deemed impractical due to its time-consuming nature, high computational costs, and substantial network usage.

A more recent and promising solution involves the implementation of Searchable Encryption (SE), wherein data remains encrypted even during operations [2]. Various SE schemes, including Homomorphic Encryption (HE), enable operations on encrypted data without exposing plaintext. HE stands out by allowing additions or multiplications on en-crypted numbers while stored in an untrusted server. Despite its potential, HE poses challenges such as heavy memory and computation costs, particularly evident in the processing of complex datasets.

Concerns about the efficiency of HE, especially in comparison to unencrypted data, have been raised, with some citing significant slowdowns in processing speed, particularly for intricate datasets like Magnetic Resonance Images (MRIs). The limitations of HE in handling such complex data suggest a need for alternative solutions. Nevertheless, the research landscape on Homomorphic Encryption is expansive, with over 51,000 related articles on Google Scholar, indicating sustained interest and exploration in the field.

This paper delves into the functionality of Searchable Encryption, including its subset Homomorphic Encryption, for the years 2019 to 2023.

1.1. Cloud and Security

The ubiquity of the Cloud as a massive infrastructure for storing and retrieving data raises concerns about the privacy of sensitive information [3]. Encryption schemes have been developed to address these concerns, as both organizations and individuals increasingly rely on the Cloud to store valuable data.

For example, airports leverage Cloud Services to enhance profitability by automating operations and integrating with IoT, sensors, GPS, surveillance cameras, and facial recognition. However, this dependence on the cloud makes the airline industry susceptible to cyber-attacks [4]. Reports indicate that a substantial portion (80%) of cloud users store sensitive data, including employee and customer information, financial records, and trade secrets [8]. Security threats such as phishing, ransomware, data leakage, and theft underscore the potential risks associated with cloud-based data storage.

In the healthcare sector, where data breaches can have severe consequences, 55% of healthcare organizations have experienced such incidents. The aftermath of a breach often requires companies to protect consumers, with services like IDX offering credit monitoring as a remedy. Research from IDX highlights various causes of data breaches, including stolen credentials, phishing, cloud misconfigurations, vulnerabilities in third-party software, and malicious insiders [5].

Despite the advantages of cloud usage, such as data availability, reduced business costs, and extensive storage space, the inherent risks of unauthorized access, data breaches, and insider threats persist [3].

1.2. Security Measures

To safeguard sensitive data, encryption is imperative. Various encryption schemes, including secure search, private information retrieval (PIR), and searchable encryption (SE), are available [3]. Data protection encompasses three key areas: data "in transit" during internet transmission, data "at rest" stored in memory or storage, and data "in use" during operations such as creation, reading, updating, deletion, or searching. All three states demand robust protection.

2. Searchable Encryption

Searchable encryption proves to be versatile by enabling operations on encrypted data without the need for decryption to plaintext. This capability is particularly advantageous for securing data in the Cloud during storage, transmission, and usage.

The inception of searchable encryption dates to 2000, with Song et al. proposing a privacy-centric approach in which untrusted servers only handle encrypted data, avoiding decryption on the server side [2]. Although this approach sacrifices some functionality, it ensures that data remains encrypted even during searches, contributing significantly to security and privacy. In this model, an attacker gaining access to the server would encounter only ciphertext, reducing the risk of unauthorized data exposure. The server remains oblivious to the actual content of the stored data, maintaining privacy during search operations. In searchable encryption schemes, servers never receive plaintext or decryption keys for any operation. To enforce this, data owners encrypt the data before uploading it to the server.

Users have multiple strategies to enhance data protection, such as using different keys in various locations for document encryption. Stronger security measures involve periodic key

changes, re-encryption of all documents, and ciphertext reordering [2]. These methods aim to prevent an outsourced or untrusted server from deducing the meaning of encrypted words.

Typically, the process of searchable encryption involves five key steps [6]:

1) Extract dataset features, such as keywords, from documents, often using TF-IDF for feature extraction.
2) Build a secure index with these keywords.
3) Encrypt the dataset.
4) Generate a search trapdoor, an encrypted query.
5) Search the index and retrieve the results.

Ongoing research explores advanced search methods, including multi-keyword searches like the Multi-Keyword Rank Searchable Encryption (MRSE) scheme based on Homomorphic Encryption, utilizing the Paillier cryptosystem with the Threshold Decryption (PCTD) algorithm [7], an indexed-based search scheme.

2.1. Searchable Symmetric Encryption (SSE)

Searchable Symmetric Encryption (SSE) exemplifies a symmetrical type of Searchable Encryption (SE) scheme. It employs a symmetric key for data encryption, allowing authorized users to search encrypted data using specific keywords or search terms. Upon conducting a search, the results are returned in encrypted form [8]. The authorized user utilizes their key to decrypt and access the information.

2.2. Public Key Searchable Encryption (PKSE)

Public Key Searchable Encryption (PKSE) represents another prevalent type of searchable encryption scheme, operating asymmetrically. In this approach, both the data and keywords are encrypted using the public key. The encrypted keywords are then sent to the server, which utilizes its private key to search the encrypted data and return the results. The outcomes are subsequently delivered to the user in encrypted form [8].

2.3. Attribute-Based Encryption (ABE)

Attribute-Based Encryption (ABE) employs fuzzy identification to implement fine-grained data access control, addressing scenarios where data owners cannot directly enforce access controls on outsourced data. ABE allows fine-grained access control, enabling specific individuals to access designated encrypted files. Additionally, ABE supports encrypted data searches using searchable encryption algorithms, facilitates file updating, and accommodates attribute revocations [8].

2.4. Order-Preserving Encryption (OPE)

Order-Preserving Encryption (OPE) is a searchable encryption scheme that enables comparisons over encrypted data. It maintains the order of ciphertexts in the same sequence as that of their plaintext counterparts. Consequently, if plaintext 1 is greater than plaintext 2, then Encrypted (plaintext 1) is greater than Encrypted (plaintext 2). OPE facilitates operations like comparisons, ordering, ranking, and range queries over encrypted data [9].

2.5. Homomorphic Encryption (HE)

Homomorphic Encryption (HE) is an encryption scheme that permits operations on encrypted data without the need for decryption [10]. Fully Homomorphic Encryption (FHE), a relatively recent variant, allows unlimited mathematical operations, primarily addition and multiplication, on encrypted data. FHE ensures the encryption, analysis, and processing of ciphertext without exposing it in decrypted form. The technique leverages bootstrapping, a process involving decryption and re-encryption after each operation, to control the growth of "noise" in the encryption scheme [10, 11].

1) Types of Homomorphic Encryption: Homomorphic En-cryption comprises various types, each offering distinct levels of functionality:

Partially Homomorphic Encryption (PHE): PHE, dating back to 1978, is widely used and allows specific mathematical operations on encrypted data, such as addition or multiplication. However, it is limited to one type of operation and is considered less secure compared to other schemes [12].

Somewhat Homomorphic Encryption (SHE): Introduced in 1978, SHE can perform both addition and multiplication operations. However, the number of homomorphic operations is limited, and additional operations introduce more noise, affecting accuracy [10].

Fully Homomorphic Encryption (FHE): Proposed by Dr. Craig Gentry in 2009, FHE allows an unlimited number of additions and multiplications on encrypted ciphertext. It employs bootstrapping to control the growth of noise, enabling operations without exposing decrypted data. Although powerful, FHE involves high computational costs and large ciphertexts [10, 11].

Research has extended the concept of Homomorphic En-cryption, leading to various modifications and combinations. For example, dynamic multi-word search schemes leverage Fully Homomorphic Encryption for improved efficiency [13].

2) FHE Open-Source Libraries: FHE is supported by several open-source libraries, each offering unique features and capabilities. Notable libraries include HElib, Microsoft SEAL, OpenFHE, PALISADE, HEAAN, FHEW, TFHE, FV-NFLlib, NuFHE, REDCuFHE, Lattigo, TFHE-rs, and more [14].

It is important for users to exercise caution and ensure a thorough understanding of the schemes before implementation, considering that some platforms may still be emerging or proprietary [12, 15].

3) Advantages of Homomorphic Encryption: Homomorphic Encryption offers several advantages, making it a promising solution for various applications:

Privacy Preservation in Cloud Services: Homomorphic Encryption enables secure data sharing in the cloud without compromising sensitive information.

Quantum Resistance: The encryption scheme is currently

impenetrable by quantum computers, providing an additional layer of security.

Secure Data Sharing: Businesses can securely share sensitive information on cloud storage services.

Regulatory Compliance: Homomorphic Encryption aligns with regulatory requirements, particularly in sectors like fi-nance and healthcare, where privacy is mandated by law [12].

4) Disadvantages of Homomorphic Encryption: Despite its advantages, Homomorphic Encryption comes with challenges and disadvantages:

Key Management: Securely managing decryption keys for authorized users in a widely accessible database can be com-plex.

Inflexibility: Encryption at various levels (record, attribute, or field) can introduce inflexibility, making record searches on encrypted data complex.

Computational Costs: Fully Homomorphic Encryption is known for its high computational costs, significantly slower than plaintext operations, especially for complex datasets [16, 17].

5) Understanding Homomorphic Encryption: Homomorphic encryption encompasses various complex schemes within the Searchable Encryption family. Notably, Paillier Homomorphic Encryption serves as a partial homomorphic encryption (PHE) scheme, while Pyfhel represents a Fully Homomorphic Encryption (FHE) scheme. FHE, being the latest in the SE family, is characterized by its intensive computing requirements, but research endeavors to enhance its viability.

Paillier HE stands out as a widely used asymmetric homo-morphic encryption system, which was pioneered by Pascal Paillier in 1999. It allows the addition of two ciphertexts or scalar multiplication without revealing the plaintext numbers. The scheme's operations, demonstrated on Wikipedia, provide transparency without relying on homomorphic encryption libraries, although math libraries are necessary [18].

Pyfhel HE, an open-source encryption library introduced by Ibarrondo et al., presents a Python implementation; although, FHE schemes are predominantly written in C++. It serves as a valuable tool for learning FHE, based on a Python wrapper for the C++ Microsoft SEAL Backend, implementing the BFV algorithm for integers and CKKS for operations using real numbers [19, 20]. Microsoft SEAL, an open-source homomorphic encryption library, facilitates mathematical computations on encrypted data [21]. Both Pyfhel and Microsoft SEAL enable unlimited addition and multiplication operations on encrypted data, controlling and observing noise to ensure accurate results upon decryption [22].

3. Schemes and Tools for Improved Searching Functionality

Advancements in Searchable Encryption (SE) have led to improvements in search functionality. From initial approaches that focused on single keyword searches, research has expanded to enhance efficiency and functionality across various aspects of SE:

3.1. Single Keyword Searches

Symmetrical Searchable Encryption, as proposed by Song et al., initially focused on single keyword searches. This approach efficiently searches documents by traversing the entire document for a specific word. Pairing this with specific schemes, such as Partial Homomorphic Encryption using the Paillier Cryptosystem, has demonstrated effectiveness [4].

3.2. Multiple Keyword Searches G. Searching Graphs

The evolution from single-keyword searches to multi-keyword searches has been accompanied by efforts to reduce computational overhead, increase efficiency, and enhance security. Research in this area includes the combination of multi-keyword searches with fuzzy and semantic searches, ranked searchable Attribute-Based Encryption (FEMRSABE), and access control in a cloud environment maintaining encrypted data (MRSF) [6, 23, 24].

Advancements also include multi-keyword ranked searches, returning the most relevant documents and allowing the server to infer keywords if users provide incorrect ones [25].

3.3. Ranges and Spatial Queries

Research has extended to include ranges and spatial queries, introducing applications such as geographical contexts for location-based services and the Internet of Things (IoT). This involves geometric range queries over encrypted data, enhancing the versatility of SE [3, 26, 27].

3.4. Fuzzy Keyword Searching

The recognition that most schemes support exact keyword searches has prompted exploration into fuzzy keyword searching to handle misspellings. Ongoing research aims to improve the efficiency of fuzzy searches and integrate them with other functionalities [28].

3.5. Ranked Searches and TF-IDF

The prominence of ranked searches, which return the most relevant documents based on keywords, has increased. Techniques like Term Frequency-Inverse Document Frequency (TF-IDF) are integrated into SE, enhancing the precision of search results [29].

3.6. Indexes

Indexes, as search structures, are explored to improve search performance. Index searches utilize an index structure for searching rather than conducting a sequential scan search. In a simple index structure, the data owner sends encrypted data and a keyword index to the cloud service provider. When a document is needed, a search token with a keyword is sent to

the cloud provider, which uses it to locate and retrieve the document [30]. Another approach involves building a "Secure Index" by extracting keywords from plaintext files, encrypting the plaintext with symmetric encryption, transforming keywords into trapdoors, and matching an authorized user's trapdoor to the Secure Index for search results [23].

A different type of index search is tree searches. They provide a range of searches and can be tailored to numerical data sets and incorporated into FHE schemes [23]. Tree-based searching methods offer efficiency and are used in combination with other functionalities, such as fuzzy and semantic searches.

Graphs and trees share similarities but also have differences. Graphs may or may not have leaf nodes, and they can flow in one or both directions, while trees flow in one direction and have leaf nodes. Researchers have explored hierarchical graph structures and graph searching, improving efficiency and combining graph searching with other functionalities, such as correcting misspellings in road networks or applying graphs in Industrial Internet of Things (IIoT) scenarios [31, 32].

3.7. Verifiable Searching

Verifiable SE schemes aim to ensure the legitimacy of search results, preventing potential alterations or deletions. Verification, while incurring high overhead, is crucial for maintaining data integrity, especially when dealing with un-trusted cloud servers [33]. Comprehensive verifiable schemes allow all parties involved to monitor the legitimacy of others [30]. Despite the overhead, research continues to improve the efficiency of verifiable searches.

Verifiable searching is often combined with other searchable functionalities, and some schemes may lack comprehensive verification, necessitating demonstrations of correctness and integrity [34]. Integration of verification with other functionalities ensures a more robust and secure search environment.

3.8. Image Searching

Images, which encompass personal photos and medical diagnostics, demand safeguarding. This extends to high-value images to prevent copyright infringement, as individuals seek control over their use [35]. Despite encryption, certain image retrieval techniques suffer from sub-optimal search accuracy [36-38]. The predominant focus in image searching research revolves around enhancing efficiency, speed, and accuracy.

3.9. Multiple Users

Not all platforms cater to single users; some necessitate multiple users accessing encrypted data. In fields like medicine, collaboration, data sharing, and collective intelligence are crucial for research [39]. This functionality is vital as multiple users rely on cloud storage solutions in semi-trusted server scenarios to protect personal data [40].

3.10. Bloom Filters

Bloom Filters play a crucial role in Searchable Encryption (SE). Unlike traditional search methods such as linear or binary searches, Bloom Filters offer a space-efficient probabilistic data structure for evaluating the membership of the set [41]. SE schemes incorporating Bloom Filters, termed Bloom Filter-based Searchable Encryption, exhibit high efficiency compared to schemes lacking Bloom Filters [42].

4. Other Functionalities

Several additional functionalities in encrypted data use have seen improvement without exhaustive enumeration. This encompasses semantics (words with similar meanings) [23], multiple data owners collaborating with multiple users [43], deduplication of data [44], comparison of multi-dimensional data between users without revealing the data [9], querying encrypted datasets with heterogeneous data sources [45], and clustering encrypted unstructured big data [46].

5. Conclusion

The increasing reliance on cloud services underscores the need for data protection, leading to the adoption of Searchable Encryption (SE). SE safeguards data through encryption, allowing operations on the data without exposing plaintext to untrusted servers. Research into SE is ongoing, spanning various branches and complex processes. As the exploration of SE functionalities evolves, researchers are addressing multiple aspects simultaneously, combining keywords, trees, indexes, and more.

Current research in SE goes beyond singular functions, incorporating a multitude of functionalities for diverse applications. FHE, as the latest advancement in SE, demands thorough understanding and evaluation. The paper provides insight into Paillier's HE and Pyfhel, demonstrating the complexity and accessibility of homomorphic encryption schemes.

In conclusion, progress in searching encrypted data is evident. Recent research improvements focus on combining multiple functionalities to make SE applicable to diverse scenarios. It is imperative to continue exploring encryption, considering societal justifications for data privacy. Despite claims questioning the viability of Fully Homomorphic Encryption, an objective evaluation reveals its potential benefits, especially when balancing the need for encrypted data with computational efficiency.

Abbreviations

ABE: Attribute Based Encryption
FHE: Fully Homomorphic Encryption
HE: Homomorphic Encryption

IIoT: Industrial Internet of Things
IoT: Internet of Things
OPE: Order Preserving Encryption
PKSE: Public Key Searchable Encryption
SSE: Searchable Symmetric Encryption
TF-IDF: Term Frequency-Inverse Document Frequency

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Cloud, "Compare AWS and Azure services to Google Cloud | Documentation," Sep. 2023. [Online]. Avail-able: https://cloud.google.com/docs/get-started/aws-azure-gcp-service-comparison

[2] Dawn Xiaoding Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proceeding 2000 IEEE Symposium on Security and Privacy. S&P 2000. Berkeley, CA, USA: IEEE Compute. Soc, 2000, pp. 44–55. [Online]. Available: http://ieeexplore.ieee.org/document/848445/

[3] I. Amorim and I. Costa, "Leveraging Searchable Encryption through Homomorphic Encryption: A Comprehensive Analysis," Mathematics, vol. 11, no. 13, p. 2948, Jan. 2023, number: 13 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/2227-7390/11/13/2948

[4] H. Malik, S. Tahir, H. Tahir, M. Ihtasham, and F. Khan, "A homomorphic approach for security and privacy preservation of Smart Airports," Future Generation Computer Systems, vol. 141, pp. 500–513, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X22004101

[5] I. cost, "The Cost of Data Breaches on Businesses," Sep. 2022. [Online]. Available: https://www.idx.us/knowledge-center/the-cost-of-data-breaches-on-businesses

[6] X. Dai, H. Dai, G. Yang, X. Yi, and H. Huang, "An efficient and dynamic semantic-aware multikeyword ranked search scheme over encrypted cloud data," IEEE Access, vol. 7, pp. 142855–142865, 2019.

[7] Y. Yang, X. Liu, and R. H. Deng, "Multi-User Multi-Keyword Rank Search Over Encrypted Data in Arbitrary Language," IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 2, pp. 320–334, 2020.

[8] G. Sucharitha, V. Sitharamulu, S. N. Mohanty, A. Matta, and D. Jose, "Enhancing secure communication in the cloud through blockchain assisted-cp-dabe," IEEE Access, vol. 11, pp. 99005–99015, 2023.

[9] N. Shen, J.-H. Yeh, H.-M. Sun, and C.-M. Chen, "A practical and secure stateless order preserving encryption for outsourced databases," pp. 133– 142, 2021.

[10] P. S. Pisa, M. Abdalla, and O. C. M. B. Duarte, "Somewhat homomorphic encryption scheme for arithmetic operations on large integers," pp. 1–8, 2012.

[11] C. Gentry, "Fully homomorphic encryption using ideal lattices," New York, NY, USA, p. 169–178, 2009. [Online]. Available: https://doi.org/10.1145/1536414.1536440

[12] IEEE, "What Is Homomorphic Encryption?" IEEE Digital Privacy, 2021. [Online]. https://digitalprivacy.ieee.org/publications/topics/what-is-homomorphic-encryption

[13] D. P. Rajan, S. J. Alexis, and S. Gunasekaran, "Dynamic multi-keyword-based search algorithm using modified based fully homomorphic encryption and Prim's algorithm," Cluster Computing, vol. 22, no. 5, pp. 11411–11424, Sep. 2019. [Online]. Available: https://doi.org/10.1007/s10586-017-1399-x

[14] Wikipedia contributors, "Homomorphic encryption," 2023 [Online] https://en.wikipedia.org/w/index.php?title=Homomorphicencryption&oldid=1173788916

[15] C. Dilmegani, "What is Homomorphic Encryption? Benefits & Challenges (2023)," 2023. [Online]. Available: https://research.aimultiple.com/homomorphic-encryption/

[16] W. Stallings and L. Brown, Computer Security Principles and Practice, 4th ed. NY, NY: Pearson, 2018.

[17] D. I. Cutress, "Intel to Build Silicon for Fully Homomorphic Encryption: This is Important," Mar. 2021. [Online]. Avail-able: https://www.anandtech.com/show/16533/intel-microsoft-darpa-to-build-silicon-for-fully/homomorphic-encryption-this-is-important

[18] Wikipedia contributors, "Paillier cryptosystem," Oct. 2023, [Online] https://en.wikipedia.org/w/index.php?title=Paillier_cryptosystem&oldid=1180504622

[19] A. Ibarrondo and A. Viand, "Pyfhel: PYthon For Homomorphic Encryption Libraries," in Proceedings of the 9th on Workshop on Encrypted Computing & Applied Homomorphic Cryptography, ser. WAHC '21. New York, NY, USA: Association for Computing Machinery, Nov. 2021, pp. 11–16. [Online]. Available: https://dl.acm.org/doi/10.1145/3474366.3486923

[20] A. Catalfamo, A. Celesti, M. Fazio, and M. Villari, "A homomorphic encryption service to secure data processing in a cloud/edge continuum context," pp. 55–61, 2022.

[21] "Microsoft SEAL (release 4.1)," https://github.com/Microsoft/SEAL, Jan. 2023, Microsoft Research, Redmond, WA.

[22] A. Ibarrondo, "ibarrond/Pyfhel," Oct. 2023, original-date: 2017-06-12T04: 15: 07Z. [Online]. Available: https://github.com/ibarrond/Pyfhel

[23] J.-K. Lin, W.-T. Lin, and J.-L. Wu, "Flexible and efficient multi-keyword ranked searchable attribute-based encryption schemes," Cryptography, vol. 7, no. 2, p. 28, May 2023. [Online]. Available: http://dx.doi.org/10.3390/cryptography7020028

[24] J. Li, J. Ma, Y. Miao, R. Yang, X. Liu, and K.-K. R. Choo, "Practical multi-keyword ranked search with access control over encrypted cloud data," IEEE Transactions on Cloud Computing, vol. 10, no. 3, pp. 2005– 2019, 2022.

[25] J. Liu, B. Zhao, J. Qin, X. Zhang, and J. Ma, "Multi-Keyword Ranked Searchable Encryption with the Wildcard Keyword for Data Sharing in Cloud Computing," The Computer Journal, vol. 66, no. 1, pp. 184–196, Oct. 2021, [Online]. Available: https://doi.org/10.1093/comjnl/bxab153

[26] Z. Gong, J. Li, Y. Lin, J. Wei, and C. Lancine, "Efficient privacy-preserving geographic keyword boolean range query over encrypted spatial data," IEEE Systems Journal, vol. 17, no. 1, pp. 455–466, 2023.

[27] X. Li, Y. Zhu, J. Wang, and J. Zhang, "Efficient and secure multi-dimensional geometric range query over encrypted data in cloud," Journal of Parallel and Distributed Computing, vol. 131, pp. 44–54, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0743731518306294

[28] M. Li, G. Wang, S. Liu, and J. Yu, "Multi-keyword Fuzzy Search over Encrypted Cloud Storage Data," Procedia Computer Science, vol. 187, pp. 365–370, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050921008693

[29] D. Sharma, "Searchable encryption: A survey," Information Security Journal: A Global Perspective, vol. 32, no. 2, pp. 76–119, Mar. 2023, publisher: Taylor & Francis [Online]. Available: https://doi.org/10.1080/19393555.2022.2033367

[30] W. Yan and S. Ji, "A secure and efficient DSSE scheme with constant storage costs in smart devices," Cyber Security and Applications, vol. 1, p. 100006, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2772918422000066

[31] S. J. Rajesh Bingu and N. Srinivasu, "Security and privacy preservation using constructive hierarchical data-sharing approach in cloud environment," Information Security Journal: A Global Perspective, vol. 0, no. 0, pp. 1–15, 2022, publisher: Taylor & Francis [Online]. Available: https://doi.org/10.1080/19393555.2022.2128942

[32] X. Ge, J. Yu, and R. Hao, "Privacy-preserving graph matching query supporting quick subgraph extraction," pp. 1–15, 2023.

[33] X. Li, Q. Tong, J. Zhao, Y. Miao, S. Ma, J. Weng, J. Ma, and K.-K. R. Choo, "Vrfms: Verifiable ranked fuzzy multi-keyword search over encrypted data," IEEE Transactions on Services Computing, vol. 16, no. 1, pp. 698–710, 2023.

[34] G. Duan and S. Li, "Verifiable and Searchable Symmetric Encryption Scheme Based on the Public Key Cryptosystem," 2023. [Online]. Available: https://www.mdpi.com/2079-9292/12/18/3965

[35] J. Widmer, "What I Learned About Copyright Law from an $800 Violation | Fluxe Digital Marketing," Sep. 2017, section: Content Marketing. [Online]. Available: https://fluxedigitalmarketing.com/what-i-learned-about-image-copyright-law-from-violation/

[36] Y. Li, J. Ma, Y. Miao, H. Li, Q. Yan, Y. Wang, X. Liu, and K.-K. R. Choo, "Dvrei: Dynamic verifiable retrieval over encrypted images," IEEE Transactions on Computers, vol. 71, no. 8, pp. 1755–1769, 2022.

[37] Y. Li, J. Ma, Y. Miao, Y. Wang, T. Yang, X. Liu, and K.-K. R. Choo, "Traceable and controllable encrypted cloud image search in multi-user settings," IEEE Transactions on Cloud Computing, vol. 10, no. 4, pp. 2936–2948, 2022.

[38] M. Navaneetha Krishnan, Mariappan A, Nithya Prasanth G, Kowsick M, and Kishore S, "Secure and search efficient information retrieval over encrypted cloud data," Journal of Survey in Fisheries Sciences, vol. 10, no. 4S, pp. 1669–1684, Apr. 2023, number: 4S Available: https://sifisheriessciences.com/journal/index.php/journal/article/view/1301

[39] M. Ali, H. He, A. Hussain, M. Hussain, and Y. Yuan, "Efficient Secure Privacy Preserving Multi Keywords Rank Search over Encrypted Data in Cloud Computing," Journal of Information Security and Applications, vol. 75, p. 103500, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214212623000844

[40] F. Ye, X. Dong, J. Shen, Z. Cao, and W. Zhao, "A verifiable dynamic multi-user searchable encryption scheme without trusted third parties," pp. 896–900, 2019.

[41] GeekstoGeeks, "Bloom Filters - Introduction and Implementation," Apr. 2017, section: Python. Available: https://www.geeksforgeeks.org/bloom-filters-introduction-and-python-implementation/

[42] Y. Liang, J. Ma, Y. Miao, D. Kuang, X. Meng, and R. H. Deng, "Privacy-preserving bloom filter-based keyword search over large encrypted cloud data," IEEE Transactions on Computers, vol. 72, no. 11, pp. 3086–3098, 2023.

[43] Y. Wang, A. Hassan, F. Liu, Y. Guan, and Z. Zhang, "Secure string pattern query for open data initiative," Journal of Information Security and Applications, vol. 47, pp. 335–352, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S221421261830382X

[44] P. Swathika and J. R. Sekar, "Time-conserving deduplicated data retrieval framework for the cloud computing environment," Automatika, vol. 64, no. 4, pp. 681–688, 2023, publisher: Taylor & Francis [Online]. Available: https://doi.org/10.1080/00051144.2023.2211439

[45] X. Feng, J. Ma, S. Liu, Y. Miao, X. Liu, and K.-K. R. Choo, "Trans-parent ciphertext retrieval system supporting integration of encrypted heterogeneous database in cloud-assisted iot," IEEE Internet of Things Journal, vol. 9, no. 5, pp. 3784–3798, 2022.

[46] S. Zobaed, S. Ahmad, R. Gottumukkala, and M. A. Salehi, "Clustcrypt: Privacy-preserving clustering of unstructured big data in the cloud," pp. 609–616, 2019.